

Formation : Palo Alto Networks - Cortex XDR: Security Operations and Integration

Cours officiel, préparation aux examens Palo Alto Networks

Cours pratique - 3j - 21h00 - Réf. PA4

Prix : 2910 € H.T.

NEW

Avec cette formation, vous développez une expertise approfondie de Cortex XDR en acquérant des compétences pratiques en opérations de sécurité, investigation d'incidents et optimisation des systèmes. Vous apprenez à comprendre le rôle des composants de la plateforme, à utiliser XQL pour analyser les données et détecter les menaces, à concevoir des workflows efficaces et à appliquer des mécanismes avancés pour renforcer les politiques de sécurité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- ✓ Expliquer le rôle et l'interaction des composants de Cortex XDR dans la protection des systèmes et des réseaux
- ✓ Utiliser le langage XQL pour interroger, analyser les journaux et détecter les menaces
- ✓ Concevoir et mettre en œuvre des workflows afin d'optimiser les opérations de sécurité
- ✓ Configurer et gérer les indicateurs et listes dynamiques pour appliquer les politiques de sécurité
- ✓ Optimiser les opérations SOC grâce à la configuration des intégrations de sécurité et des tableaux de bord XDR

Public concerné

Ingénieurs et responsables SOC / CERT / CSIRT / XDR, MSSP et partenaires de services ou intégrateurs de systèmes, ainsi que consultants en cybersécurité et ingénieurs avant-vente sécurité.

Prérequis

Solide compréhension des principes de la cybersécurité, notamment des concepts de sécurité réseau et endpoint. Bonne compréhension de l'anglais à l'écrit.

PARTICIPANTS

Ingénieurs et responsables SOC / CERT / CSIRT / XDR, MSSP et partenaires de services ou intégrateurs de systèmes, ainsi que consultants en cybersécurité et ingénieurs avant-vente sécurité.

PRÉREQUIS

Solide compréhension des principes de la cybersécurité, notamment des concepts de sécurité réseau et endpoint. Bonne compréhension de l'anglais à l'écrit.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.

Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.

Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...

À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

- 1 Module 1 : Présentation de Cortex XDR
- 2 Module 2 : Composants logiciels
- 3 Module 3 : Intégrations
- 4 Module 4 : XQL
- 5 Module 5 : Ingénierie de la détection
- 6 Module 6 : Automatisation de la plateforme
- 7 Module 7 : Optimisation du système
- 8 Module 8 : Tableaux de bord et rapports
- 9 Module 9 : Sécurité de la messagerie

Options

Certification : 260 € HT

Palo Alto Networks Certified XDR Engineer

[Comment passer votre examen ?](#)

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE

2026 : 24 mars, 16 juin, 22 sep., 24 nov.

PARIS LA DÉFENSE

2026 : 23 mars, 24 mars, 24 nov.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.